Vlaamse overheid

Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer

Advies VTC nr. 02/2018 van 18 april 2018

<u>Betreft</u>: Vraag om advies inzake de encryptiebouwsteen van het Facilitair Bedrijf voor het hosting door Amazon Web Services.

De Vlaamse Toezichtcommissie (hierna: "de VTC");

1. Gelet op het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (hierna: "het e-govdecreet"), inzonderheid artikel 9 en 11;

2. Gelet op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna: "WVP");

3. Gelet op de wet van 5 mei 2014 houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren (hierna "wet van 5 mei 2014"), inzonderheid artikel 5;

4. Gelet op het verzoek om advies van het Facilitair Bedrijf, ontvangen op 14 maart 2018 per mail;

5. Gelet op de voorstelling van 23 maart 2018 en bespreking op de zitting van de VTC van 18 april 2018;

6. Brengt op 18 april 2018 het volgend advies uit:

<u>I. ONDERZOEK</u>

7. Het uitgangspunt is dat de partij die de hosting doet geen toegang heeft tot leesbare data.

8. De VTC verwijst naar de powerpoint bij de presentatie van 23 maart 2018.

9. Tijdens de presentatie werden de volgende hoofdpunten belicht:

10. De vraag wordt voorgelegd in het kader van het **model van informatieclassificatie** dat het Facilitair Bedrijf aan het uitwerken is. De bouwsteen "Encryptie op AWS" voor *data at rest* (DAR) wordt als een algemene minimale maatregel voor informatie ingedeeld in de klasse 4.

11. De bouwsteen werd uitgewerkt voor het project 'burgerloket' (of 'burgerprofiel' - zie machtiging VTC/42/2017) en is ook van toepassing het project hosting van de LED (zie advies VTC/A/01/2018) omdat dat POC's zijn voor de informatie classificatie waarvoor Facilitair Bedrijf een model uitwerkt. Deze encryptiebeheersdienst (AWS KMS) zal worden aangeboden aan alle projecten binnen de AWS context[1].

12. Tijdens de behandeling van de adviesvraag werd verduidelijkt[2] dat encryptie voor *data at rest* voor wat het gebruik van AWS betreft ook zal toegepast worden bij klasse 3 (vertrouwelijke) informatie.

13. Het Facilitair Bedrijf heeft daarbij gesteld dat de encryptie van *data at rest* volgens het informatie classificatiemodel van het Facilitair Bedrijf niet verplicht is voor klasse 3. Het Facilitair Bedrijf zal één enkel proces aanbieden afgestemd op klasse 4. In het geval dat encryptie zal worden toegepast op klasse 3 (of lager) dan zal ditzelfde proces/uitwerking worden gebruikt. Het is niet rendabel om speciaal voor klasse 3 een apart proces in te regelen. (zie verder voor commentaar VTC)

14. Het voorgestelde betreft **enkel de technische uitwerking**. Hoe bv. de sleutels gebruikt worden valt onder de verantwoordelijkheid van de beheerder van de applicatie.

15. De voorgestelde bouwsteen geldt enkel voor ***data at rest*** (en dus niet automatisch voor *data in use* (DIU) waarbij encryptie moet worden ingebouwd in de code). (Voor data in motion (DIM) is er *end-to-end* encryptie;[3])

16. Met het voorstel wordt tegemoet gekomen aan de voorwaarde van de VTC (aanbeveling VTC/AB/2016/01) dat encryptiesleutels onder het beheer van de verantwoordelijke (of een trusted third party) moeten zijn: bij de voorgestelde maatregel zijn de **sleutels onder beheer** (incl. transport en gebruik ervan) **van de VO** (Facilitair Bedrijf sleutelbeheersdienst). Het sleutel**gebruik** valt onder de verantwoordelijkheid van de beheerder van de toepassing. Dit is een toepassing van scheiding van functies.

17. Er wordt een **standaard AWSprocedure** gevolgd waarbij gebruik wordt gemaakt van de Key Management Service van AWS met een Customer Managed Key.

18. De sleutelrotaties zijn volledig dynamisch.

[1] Bv Ondernemersloket wil ook gebruik maken van deze dienst
[2] Het model van informatiedataclassificatie dat aan de VTC werd getoond in 2017 sprak bij klasse 3 (vertrouwelijke gegevens) over *'voor data at rest enkel endpointencryptie als verplicht en andere encryptie aanbevolen'.* Dit is dus gewijzigd intussen voor wat AWS betreft. (met endpointencryptie wordt encryptie op de werkplek/portable bedoeld)
[3] Er wordt aan gedacht die in te voeren voor alle informatieklassen (om integriteitsredenen).

19. De door de VTC opgeworpen problematiek van het **risico dat data worden bijgehouden totdat decryptie mogelijk is met verouderde sleutels** wordt zeer sterk beperkt doordat er regelmatig herencrypteerd wordt en de sleutel (meerdere sleutels eigenlijk) niet bij de data wordt bewaard. Dit blijft niettemin een risico voor longitudinale gegevens.

20. Er is echter een strikte opvolging van de historische sleutels, waardoor het risico zoveel mogelijk wordt ingeperkt.

21. Het **toegangsbeheer** wordt niet gedaan door AWS. Dit zit volledig bij de Vlaamse overheid (het Vlaamse ACM/IDM beheerd door het Facilitair Bedrijf). Dit is ook een toepassing van scheiding van functies. Bij elke sleutel die gegenereerd wordt hangt een policy waarin staat wie die sleutel mag gebruiken. Er kan ook niets gedaan worden met de sleutel alleen en AWS heeft nooit de sleutel.

22. Daarnaast wordt ook **Priviliged Acces Management** (PAM) geïmplementeerd waardoor alle handelingen nauwkeurig worden bijgehouden zodat men perfect weet wie wat heeft gedaan.

II. BESLUIT

23. De VTC herinnert er aan dat in het geval persoonsgegevens verwerkt worden in een externe cloudomgeving , zoals bij AWS (tegenover een *on premise community cloud*), de gegevens altijd moeten geëncrypteerd worden van zodra ze niet in de categorie publiek vallen, dus ook voor klasse 3, want zonder encryptie heeft men geen controle meer.

24. De VTC stelt vast dat men inspanningen doet om regelmatig te herencrypteren. Eigenlijk zou men moeten zorgen dat dit in de hardware ingebed wordt. Nu hangt alles af van de concrete implementatie. De gebruikte methodologie is wel correct.

25. Het consulteren van een databank houdt in dat minstens de metadata gedecrypteerd worden. Het gaat dus om meer dan *data at rest*. Op het moment van vercijfering draaien programma's die deze gegevens zien.

26. De hele virtuele omgeving van AWS wordt wel vercijferd t.o.v. AWS, maar daarom moet steeds ook herencrypteerd worden.

27. Homomorfe encryptie voor *data in use*, die het mogelijk maakt (bepaalde) berekeningen te maken op versleutelde gegevens, staat vandaag niet op punt (weinig performant).

28. De VTC is van oordeel dat de in de presentatie geschetste encryptiemaatregel in de voorgestelde context (zie machtiging burgerloket en advies LED) een maatregel is, die voldoende betrouwbaar is.

29. De VTC beveelt aan dat de dynamische encryptie door alle overheden kan gebruikt worden.

De voorzitter,
Willem Debeuckelaere